Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2014/005

Audit of information and communications technology management at the International Criminal Tribunal for the former Yugoslavia

Overall results relating to the effectiveness of information and communications technology management were initially assessed as partially satisfactory. Implementation of seven important recommendations remains in progress.

FINAL OVERALL RATING: PARTIALLY SATISFACTORY

26 February 2014
Assignment No. AA2013/270/02

CONTENTS

AUDIT REPORT

Audit of information and communications technology management at the International Criminal Tribunal for the former Yugoslavia

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of information and communications technology (ICT) management at the International Criminal Tribunal for the former Yugoslavia (ICTY or Tribunal).

2. In accordance with its mandate, OIOS provides assurance and advice on the adequacy and effectiveness of the United Nations internal control system, the primary objectives of which are to ensure (a) efficient and effective operations; (b) accurate financial and operational reporting; (c) safeguarding of assets; and (d) compliance with mandates, regulations and rules.

3. ICTY was established in 1993 as a temporary institution with a mandate of investigating crimes committed during the wars in the former Yugoslavia and prosecuting those responsible. The Mechanism for International Criminal Tribunals (MICT or Mechanism) was established by the United Nations Security Council on 22 December 2010 to carry on a number of essential residual functions of the International Criminal Tribunal for Rwanda (ICTR) and ICTY after the completion of their respective mandates, and was comprised of two branches: The Hague and Arusha. Until 31 December 2013, the Mechanism did not have its own administrative services and relied on ICTY and ICTR to provide administrative support, including ICT management, at both branches.

4. The ICTY Information Technology Services Section (ITSS) was responsible for providing ICT services in support of the Tribunal and Mechanism's operations, including maintenance, administrative management, training, technical and end-user assistance to all systems in key business and administrative areas based in The Hague and in field offices in Sarajevo and Belgrade. ITSS was part of the Registry in the Division of Administration.

5. ITSS was staffed with 47 staff members (eight Professional and 39 General Service staff), and headed by the Chief of Section at P-5 level, who reported to the Chief Administrative Officer. ICTY budgets and ICT expenditure for the biennia 2010-2011 and 2012-2013 (as of September 2013) are shown in Table 1 below. Additionally, in the context of ICT management services provided to the Mechanism, from January 2012 to September 2013, ICTY disbursed approximately $2.1 million on behalf of MICT, The Hague branch. ITSS also played a strategic role in the development of the ICT foundation for MICT and was leading a project of $3.1 million at the time of the audit for that purpose.

Table 1: ICTY budgets and ICT expenditure (in $ million)

	2010-2011	2012-2013*	Total
ICTY consolidated budget	**320.5**	**280.2**	**600.7**
ICTY ICT expenditure	**7.7**	**6.1**	**13.8**
Acquisitions of equipment and software	3.5	1.8	5.3
Communications and data processing	2.0	1.6	3.6
Maintenance services	1.8	2.2	4.0
Supplies	0.4	0.5	0.9

* Expenditure as of September 2013
Source: ICTY Management Report, 18 September 2013

6. Comments provided by ICTY are incorporated in *italics*.

II. OBJECTIVE AND SCOPE

7. The audit was conducted to assess the adequacy and effectiveness of ICTY governance, risk management and control processes in providing reasonable assurance regarding the **effective management of ICT at ICTY**.

8. OIOS included the audit in its 2013 work plan because of the risks stemming from the fact that ICT systems were critical to ensure the successful completion of the ICTY mandate and in supporting the operations of MICT.

9. The key controls tested for the audit were: (a) Risk management and strategic planning mechanisms; (b) Project management capacity; and (c) ICT support systems. For the purpose of this audit, OIOS defined these key controls as follows:

(a) **Risk management and strategic planning mechanisms** – controls that provide reasonable assurance that risks relating to ICT systems are identified and assessed, and that action is taken to mitigate them.

(b) **Project management capacity** – controls that provide reasonable assurance that there is sufficient project management capacity to achieve mandates, including: (i) sufficient financial resources; (ii) sufficient and competent human resources; and (iii) appropriate project management tools, methodology and systems.

(c) **ICT support systems** – controls that provide reasonable assurance that the ICT systems are adequately supporting the business objectives of ICTY.

10. The key controls were assessed for the control objectives shown in Table 2. Certain control objectives (shown in Table 2 as "Not assessed") were not relevant to the scope defined for this audit.

11. OIOS conducted this audit from 1 May 2013 to 30 October 2013. The audit covered the period from 1 January 2011 to 31 March 2013.

12. OIOS conducted an activity-level risk assessment to identify and assess specific risk exposures, and to confirm the relevance of the selected key controls in mitigating associated risks. Through interviews, analytical reviews and tests of controls, OIOS assessed the existence and adequacy of internal controls and conducted necessary tests to determine their effectiveness.

III. AUDIT RESULTS

13. ICTY governance, risk management and control processes examined were assessed as **partially satisfactory** in providing reasonable assurance regarding the **effective management of ICT at ICTY**. OIOS made seven recommendations to address issues identified in the audit. ICTY had established an ICT governance structure to oversee ICT projects. However, it needed to enhance this structure by: clarifying the roles and responsibilities of the ICT Committee in the approval of ICT projects of ICTY and MICT; clarifying the criteria for assessing MICT ICT projects; and reviewing and approving the ICTY ICT strategy to incorporate a clear definition of ICT priorities and investments for the completion of ICTY mandate and transfer to MICT. Project management activities needed strengthening to ensure effective contribution and alignment of ICT projects with the ICT strategy/priorities by providing:

adequate business justification for projects; quantification of projects' intended benefits and resources needed for implementation; information security compliance reviews on intended ICT solutions; and effective monitoring of costs and milestones during project implementation. ICTY also needed to assess the achievement of intended project benefits through post-implementation reviews. Portfolio management practices required strengthening through the implementation of a catalogue of applications to support identification of redundant applications and reduction of the overall portfolio in preparation for the closure of the Tribunal. Additionally, ICTY needed to address inadequate access to systems' information granted to certain users and to improve recording of software licenses and internally developed software to meet reporting requirements under International Public Sector Accounting Standards (IPSAS) on intangible assets.

14. The initial overall rating was based on the assessment of key controls presented in Table 2 below. The final overall rating is **partially satisfactory** as implementation of seven important recommendations remains in progress.

Table 2: Assessment of key controls

Business objective	**Key controls**	**Control objectives**			
		Efficient and effective operations	**Accurate financial and operational reporting**	**Safeguarding of assets**	**Compliance with mandates, regulations and rules**
Effective management of ICT at ICTY	(a) Risk management and strategic planning mechanisms	Partially satisfactory	Satisfactory	Partially satisfactory	Partially satisfactory
	(b) Project management capacity	Partially satisfactory	Partially satisfactory	Partially satisfactory	Not assessed
	(c) ICT support systems	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
FINAL OVERALL RATING: PARTIALLY SATISFACTORY					

A. Risk management and strategic planning mechanisms

There was a need to clarify the roles and responsibilities of the ICT Committee

15. ICTY established an ICT strategy for the Tribunal and an ICT Committee as part of its ICT governance structure. This was in line with the governance structure described in the Secretary-General's report A/62/793 for implementing the ICT strategy of the Secretariat, which included management oversight committees and advisory bodies providing advice on ICT initiatives to ensure alignment of ICT with the organization's mandates and objectives and promotion of responsible use of ICT resources.

16. The audit showed instances where the ICT Committee performed functions beyond its terms of reference, and in some cases there was lack of clarity regarding its roles and responsibilities, as explained below:

a. According to the terms of reference, the ICT Committee had the responsibility of advising the Registrar on ICT investments after assessing and prioritizing project proposals in line with the strategic objectives of ICTY, as reflected in the ICT strategy. However, despite its advisory role to the Registrar, the Committee was approving projects, and therefore making decisions on the use of ICT resources of both ICTY and MICT.

b. In line with the framework for administrative support provided by ICTY to the establishment of MICT, ITSS led a $3.1 million project for the establishment of MICT ICT infrastructure at both its branches. The on-going project (divided into three smaller projects: MICT Infrastructure, MICT Virtual Private Network, and MICT Substantial Systems) was submitted to the ICT Committee for prioritization and also for decision on which systems were required for MICT operation. However, there was no delegation of authority to the ICTY ICT Committee to prioritize MICT projects and to make decisions on systems to be used by MICT. Also, while criteria were defined for the prioritization of ICT projects of ICTY, no criteria were defined for the prioritization and decision on ICT projects of MICT, as the ICT strategy for MICT was not defined.

17. ICTY explained that senior management had access to the minutes of the ICT Committee meetings and had the power to vet the decisions made by the Committee. ICTY also explained that the role of the ICTY ICT Committee in the assessment of ICT projects of MICT was assumed within the obligation of the Tribunal to provide administrative support to MICT, but acknowledged the need to clarify the criteria for prioritization of MICT ICT resources. Lack of clarity in the roles and responsibilities of the ICTY ICT committee could have an adverse impact on accountability and effective use of ICT resources.

(1) ICTY should clarify: (a) the roles and responsibilities of the ICT Committee; and (b) the criteria for assessing ICT investments of MICT, in coordination with MICT.

ICTY accepted recommendation 1 and stated that it will update and re-circulate the terms of reference of the ICT Committee. Also, a proposal will be sent to the MICT Registrar that he officially appoint adequate MICT representation in the joint ICT Committee and recognize the advice of the Committee, acting in a joint organizational capacity, to make recommendations to him on MICT ICT projects and related expenditure. Recommendation 1 remains open pending receipt of the updated terms of reference and membership of the ICT Committee, and clarification of the criteria to be used to prioritize MICT ICT projects.

There was a need to improve ICT planning and monitoring

18. The ICTY ICT strategy was an essential tool for ensuring alignment of ICT investments with the Tribunal's business needs during the completion of its mandate and provision of administrative support to MICT. The ICT strategy was still in draft form at the time of audit and had not been endorsed by the ICT Committee or approved by senior management.

19. There were weaknesses in the formulation and implementation of the ICT strategy in that the strategy referred to generic organizational goals (i.e., completion of the ICTY mandate and support for transfer to MICT), but did not identify the related ICT priorities and resources. Also, although the overall resource requirements were quantified in the budget, there was no visible connection between the ICT strategy and the budget. The strategy cascaded into discrete ICT projects whereas the budget quantified ICT resource requirements under various budget lines, mixing both new investments and the cost of providing day-to-day services. Further, the strategy was not reviewed on an annual basis, as required by the terms of reference of the ICTY ICT Committee. Periodic reviews were necessary to ensure the continued alignment of the strategy with the organization's mandate, business needs, shifting priorities, technological developments, and available resources.

20. ICTY explained that there were difficulties in setting ICT priorities up front, as these kept evolving and there was a need to implement a reactive approach to upcoming business requests. ICTY attributed the lack of endorsement, approval and periodic review of the ICT strategy to conflicting priorities of relevant stakeholders. Shortcomings in the definition and endorsement of strategic priorities led to lack of engagement of stakeholders in the execution of the strategy and diminished the effectiveness of ITSS in managing its resources.

(2) ICTY should revise and formally approve its ICT strategy in order to identify ICT priorities and the resources required for completing its mandate and transfer/support to MICT.

ICTY accepted recommendation 2 and stated that it will review and formally approve its ICT strategy. Recommendation 2 remains open pending receipt of the updated and approved ICT strategy.

B. Project management capacity

There was a need to enhance project formulation, monitoring and post-implementation assessments

21. In line with recommended practice for the United Nations Secretariat, ICTY adopted PRINCE2 (Projects in Controlled Environments) and Information Technology Infrastructure Library (ITIL) principles in the governance and management of its ICT projects. The project governance framework included: project proposals formalized by business owners through a pre-defined business case template and detailed project plans; prioritization of ICT projects by the ICT Committee; designation of project stakeholders (sponsors, business owners, project managers, project boards, business representative teams, and development teams); designation of Change/Emergency Change Advisory Boards within the ITIL change management process to assess the impact of project implementation on existing systems and services prior to project deployment; and development of relevant technical and operational documentation for systems and applications.

22. From January 2011 to March 2013, ICTY launched 27 projects of which 15 were reviewed by the ICT Committee after this committee was re-established in January 2012. OIOS conducted a high level review of the 15 projects presented to the ICT Committee (focusing on cost elements) and a more detailed review of 12 projects (focusing on the overall project management cycle). Several weaknesses relating to project planning, monitoring and documentation were highlighted from the review, as follows:

a. Insufficient business justification: Business cases justified projects generally in the context of the broad goals of ICTY mandate, completion strategy and transfer/support to MICT, leading to nearly all project proposals being accepted with this minimum justification. Also, the effective contribution of projects to the generic organizational goals was not systematically identified, with only four out of 12 project proposals reviewed by OIOS providing some quantification in terms of relevant efficiency gains which would accrue from the relevant projects.

b. Lack of identification of project interdependencies: Business cases did not identify the impact of implementation of specific projects, such as in the maintenance or reduction of other systems and applications (for example, the Registry Jigsaw project for the implementation of a database of centralized witness information required several other supporting databases to be kept). Such identification was done to a limited extent in the project plans after project initiation, and more thoroughly during the change management process that preceded the deployment of new systems, applications or functionalities. However, the high-level identification of project interdependencies at project proposal stage would have aided the ICT Committee in its project assessment, specifically in the verification of the strategic objective of reducing the number and complexity of ICT services, applications and infrastructure. Also, early identification of project interdependencies would have enabled validating the projects' benefits before committing resources.

c. Inadequate quantification of resources: In the 15 projects that were submitted to the ICT Committee for review, there was either no quantification (in five projects or 33 per cent) or incomplete quantification (in 10 projects or 66 per cent) of the resources required for implementation. Consequently, there was no cost-benefit analysis to justify these projects. Also, there was no process in place to capture all relevant costs of internally generated intangible assets (development phase), to facilitate their reporting under IPSAS.

d. Limited monitoring of projects: ITSS and the Project Boards, which were appointed for each project, monitored progress of development and implementation of projects through periodic meetings and status reports prepared by project managers. Also, timely feedback on the status of on-going projects was provided by the Chief of ITSS to the ICT Committee. However, except in one out of the 12 projects reviewed, no comparison was made between planned and actual milestones and timeframes. Additionally, project costs were not monitored. Thus, it was not possible to determine project implementation delays, impact of the delays on operations, and potential cost overruns. In addition, ICTY did not conduct post-implementation reviews of any of the projects reviewed, to assess the degree of achievement of projected benefits.

e. Insufficient documentation controls: Project documents, namely business cases, project plans, project specifications, risk registers, status reports, and user acceptance documents, were not kept systematically and updated for all projects and were not signed-off by relevant stakeholders. As a result, there was inadequate evidence of agreement and approval of project conditions and deliverables to support stakeholder commitment, and monitoring and control of project delivery.

23. ICTY acknowledged the need to enhance its project management process, especially at the project proposal and post-implementation review levels. As part of the improvement efforts, ITSS introduced in 2011 mandatory training in PRINCE2 for its project managers and for other staff of the Tribunal. Nevertheless, the shortcomings in project management needed to be systematically addressed to optimize ICT project deliverables.

(3) ICTY should improve ICT project management by strengthening the formulation of project proposals, project monitoring and reporting, and maintenance of project documentation for ICT projects.

ICTY accepted recommendation 3 and stated that the ICT Committee will ensure that proposed projects are explicitly aligned with the adopted ICT strategy and the benefits, resource costs and risks are stated in the business case prior to project consideration and approval. Also, ICTY will strengthen its use of the PRINCE2 project management methodology and will maintain standard ICT project documentation commensurate with the project's size and complexity. Recommendation 3 remains open pending receipt of project documentation demonstrating alignment of project proposals with approved ICT priorities, quantification of project benefits and costs, monitoring of projects milestones and costs, and adequate project documentation.

There was a need to establish and maintain adequate inventories of applications

24. ICTY estimated to have approximately 570 systems and applications in its portfolio, of which approximately 106 were linked to main business processes and support functions. Except for software licenses, ITSS did not maintain an updated catalogue of systems for managing its portfolio of applications. Instead, repositories of applications were produced on demand to meet specific needs. Further, these ad-hoc repositories did not provide consistent information about business processes and business owners of the different applications. Data was incomplete or out-dated, and presented inconsistent criteria for the identification of applications, including: applications identified by their title in some cases, and by their title and versions in other cases; systems/applications such as Automatic Notification Agent and Procurement Notifications, which would normally be a part of other systems/applications were sometimes treated as stand-alone applications; and inconsistencies in naming conventions of systems/applications which potentially resulted in double or multiple counting. For example, designations like Procurement Contract Tracking, Procurement Notifications, Procurement Reporting, Procurement Suite and Procurement System all referred to the same system. It was therefore difficult for ICTY to determine the exact number of systems and applications in its portfolio.

25. The inconsistencies above resulted from lack of procedures and criteria for the maintenance of inventories or catalogues of applications and in the fact that the listings were consolidated from several different compilations within ITSS. Incomplete data and inconsistencies in inventories of applications impeded effective lifecycle management and identification of redundant applications. This could prevent ICTY from optimizing its ICT resources and reducing the number of systems/applications to be supported, in preparation for the closure of the Tribunal and transfer to MICT.

(4) ICTY should establish a consolidated and updated catalogue of applications and procedures for its maintenance to facilitate closure arrangements and transfer of systems to MICT.

ICTY accepted recommendation 4 and stated that it will establish a consolidated application portfolio and will adopt procedures which will ensure that the established portfolio is maintained and updated. Recommendation 4 remains open pending receipt of the consolidated application portfolio and the procedures established for its maintenance.

C. ICT support systems

There was a need to enhance information security reviews

26. The ICTY ICT infrastructure was defined in early 2000, based on information security guidelines drafted by the ICTY Security and Safety Section. The guidelines were in accordance with industry best practices provided by BS ISO/IEC 17799:2000 on Information technology - Code of practice for information security management and considered specific security requirements of the Tribunal. After this initial definition, the ICT infrastructure evolved with the implementation of new systems, applications, functionalities and access roles. The portfolio of 27 projects launched by ITSS during the audit period included initiatives such as: cloning of existing systems and applications for use by different sections in the Tribunal and MICT, enhancing of functionalities by linking information residing in different databases owned by different sections with different confidentiality requirements, and implementing free Wi-Fi in ICTY premises. Some of these initiatives had the potential to compromise information security. However, except for one project, these projects were not subjected to review by the Security and Safety Section, to ensure continued compliance with recommended information security guidelines.

(5) ICTY should ensure that ICT project proposals are subjected to information security reviews prior to their submission to the ICT Committee, to ensure compliance with information security guidelines.

ICTY accepted recommendation 5 and stated that the template used for project proposals (High Level Business Case) will be amended to ensure that each project proposal is reviewed by the Information Security Officer prior to consideration by the ICT committee. Recommendation 5 remains open pending receipt of the revised template for project proposals, incorporating the requirement for information security review.

Access rights and roles required revision

27. Section 3 of the Secretary-General's bulletin ST/SGB/2004/15 dated 29 November 2004 on the use of information and communication technology resources and data required the use of ICT resources and data consistent with the functional obligations of authorized users. Section 5 of the same bulletin defined the activities prohibited when using ICT resources and data, which could be reinforced with adequate access rights to information. During a review of 345 access rights and roles, several weaknesses were noted in the system of controls established by ICTY for regulating access to its information systems, as detailed below:

a. Nineteen users had access to the Personnel Information Management System (PIMS) and to contractual, personal and private information of staff members which was not justified in the context of the functions assigned to those users. Eleven of the 19 users had full access rights to actions and transactions in the system including "create, read, update, delete", while the remaining eight had read-only access rights. Access to contractual, personal and private information of staff members may lead to unauthorized creation, deletion, alteration or disclosure of data and breach of privacy.

b. In 39 cases reviewed, representing 11 per cent of the total, 26 users retained their prior access rights to systems after internal transfers to other functions, external transfers to MICT, or transfers due to cross-training and loans.

c. Access rights assigned to some users violated the requirement for segregation of functions and duties. For example a procurement role in the OneSource system was assigned to one staff in the Finance Section which could result in the staff performing both issuance of purchase orders and approval of accounting entries for the same purchase orders. Similarly, a human resources certifying officer role in PIMS was assigned to the Chief of Finance Section, which conflicted with the staff member's current responsibilities by allowing both certifying and approving roles. Additionally, in 10 cases, access rights to business functions belonging to various sections were assigned to six ITSS users, allowing these users to perform operational tasks in different systems. ICTY justified access of ITSS users to business functions in the context of technical support that needed to be provided to different systems and referred to the existence of access logs for some systems to keep track of users' actions. However, there were no procedures in place to review such logs to detect inappropriate transactions.

28. ICTY explained that the inadequacies in access controls to PIMS were due to system limitations and stated that a reporting tool had been developed which would prevent violations in the future. ICTY also stated that users maintained their access rights to systems due to lack of communication from Section

Managers regarding staff cross-training with other Sections or internal transfers. ICTY also explained that ITSS had taken action to revoke the access rights, but OIOS noted that the unjustified access to PIMS had not been revoked. ICTY was in the process of drafting a Standard Operating Procedure to improve access role management during internal movement of staff. Access role management and controls were necessary to maintain checks and balances as the Tribunal was downsizing and had adopted the strategy of transfers and cross-training to strengthen multi-tasking capabilities and resilience of staff.

(6) ICTY should strengthen access role management by: (a) reviewing the list of users with access to the Personnel Information Management System and the OneSource system and revoking the access rights granted to staff that no longer need to use the systems; (b) implementing standard operating procedures for managing roles and credentials for accessing information systems during the movement of staff within the Tribunal; and (c) instituting periodic reviews of access roles and logs pertaining to critical systems and applications.

ICTY accepted recommendation 6 and stated that the list of users with access to PIMS and the OneSource system will be reviewed and appropriately amended with the collaboration of Human Resources and Procurement Sections, respectively. ICTY also stated that it will publish a Standard Operating Procedure which will enable ITSS and the business owners jointly to manage user access roles. Additionally, ITSS will review access roles lists for critical systems and applications, at minimum every quarter, with business owners, and the results of the review will be documented and acted upon with minimum delay. Due to the larger amount of records automatically generated by the logs and resource overheads involved in reviewing these logs, the access logs will be reviewed only when required in the context of specific incidents. Recommendation 6 remains open pending receipt of: an amended list of users and access rights to PIMS and the OneSource system; the published Standard Operating Procedure on access roles management; and evidence of periodic review of access roles pertaining to critical systems.

Structure for software license management was in place but controls required strengthening

29. License software management functions were performed by dedicated resources within ITSS, including staff and a software management system. In addition, ITSS: established the function of the "Software manager", which was performed by an Operations Officer, to provide approvals for the purchase and issuance of software licenses based on business justifications; and documented the license issuance process. As of 18 June 2013, ICTY had 19,974 active licenses for 323 titles and versions of software. Of these, a total of 81 per cent (or 16,272) were in use and the remaining 19 per cent (or 3,702) were not used.

30. The United Nations Secretariat's guidance for IPSAS on intangible assets (IPSAS 13) dated 26 June 2013 established the criteria under which intangible assets, including externally acquired software and software licenses, were to be recognized prospectively (i.e., no recognition in the opening statement of financial position as of 1 January 2014, but subject to recognition thereafter). Software licenses acquired for a period of one year or longer should be capitalized as an intangible asset and amortized over its useful life, if they meet the capitalization threshold of $5,000 per unit/user.

31. The system used by ICTY for recording and controlling software licenses did not include relevant information for IPSAS compliance, such as cost (purchase price, import duties, and non-refundable taxes), units, and dates of purchase or use for measurement and reviewing impairment of individual licenses. The criteria used for recording the number of enterprise Original Equipment Manufacturer (OEM), site, and volume licenses were inconsistent. For example, in some cases the records did not show

the correct number of licenses, while in other cases, for the same type of license, the records showed the number of units (users or computers) that each license allowed.

32. Inadequate recording and measurement of costs and usage of software licenses did not allow effective control and acquisition/disposal planning and did not meet requirements for IPSAS compliance after 1 January 2014. ICTY attributed the shortcoming to system limitations, late issuance of guidance by the IPSAS Implementation Team at Headquarters, which resulted in lack of preparedness to deal with requirements on the reporting of intangible assets under IPSAS.

(7) ICTY should design and implement procedures for tracking all the data associated with the acquisition and/or development of software applications in preparation for compliance with the IPSAS requirements for intangible assets.

ICTY accepted recommendation 7 and stated that software acquisition data will be recorded and tracked using the Central Supplies System and that in-house developed software will be recorded in the Time Tracking application to estimate the total development cost and ensure appropriate compliance with IPSAS requirements. Recommendation 7 remains open pending receipt of documentation showing adequate recording and tracking of software-related data for compliance with IPSAS on intangible assets.

IV. ACKNOWLEDGEMENT

33. OIOS wishes to express its appreciation to the Management and staff of ICTY for the assistance and cooperation extended to the auditors during this assignment.

(*Signed*) David Kanja
Assistant Secretary-General for Internal Oversight Services

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology management at the International Criminal Tribunal for the former Yugoslavia

Recom. no.	Recommendation	Critical[1]/ Important[2]	C/ O[3]	Actions needed to close recommendation	Implementation date[4]
1	ICTY should clarify: (a) the roles and responsibilities of the ICT Committee; and (b) the criteria for assessing ICT investments of MICT, in coordination with MICT.	Important	O	Receipt of the updated terms of reference and membership of the ICT Committee, and clarification of the criteria to be used to prioritize MICT ICT projects.	30 June 2014
2	ICTY should revise and formally approve its ICT strategy in order to identify ICT priorities and the resources required for completing its mandate and transfer/support to MICT.	Important	O	Receipt of the updated and approved ICT strategy	30 June 2014
3	ICTY should improve ICT project management by strengthening the formulation of project proposals, project monitoring and reporting, and maintenance of project documentation for ICT projects.	Important	O	Receipt of project documentation demonstrating alignment of project proposals with approved ICT priorities; quantification of project benefits and costs; monitoring of projects milestones and costs; and adequate project documentation	30 June 2014
4	ICTY should establish a consolidated and updated catalogue of applications and procedures for its maintenance to facilitate closure arrangements and transfer of systems to MICT.	Important	O	Receipt of the consolidated application portfolio and the procedures established for its maintenance.	30 September 2014
5	ICTY should ensure that ICT project proposals are subjected to information security reviews prior to their submission to the ICT Committee, to ensure compliance with information security guidelines.	Important	O	Receipt of the revised template for project proposals, incorporating the requirement for information security review.	30 June 2014
6	ICTY should strengthen access role management	Important	O	Receipt of an amended list of users and access	30 April 2014

[1] Critical recommendations address significant and/or pervasive deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance cannot be provided regarding the achievement of control and/or business objectives under review.

[2] Important recommendations address important deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

[3] C = closed, O = open

[4] Date provided by ICTY in response to recommendations.

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology management at the International Criminal Tribunal for the former Yugoslavia

Recom. no.	Recommendation	Critical[1]/ Important[2]	C/ O[3]	Actions needed to close recommendation	Implementation date[4]
	by: (a) reviewing the list of users with access to the Personnel Information Management System and the OneSource system and revoking the access rights granted to staff that no longer need to use the systems; (b) implementing standard operating procedures for managing roles and credentials for accessing information systems during the movement of staff within the Tribunal; and (c) instituting periodic reviews of access roles and logs pertaining to critical systems and applications.			rights to PIMS and the OneSource system; of the published Standard Operating Procedure on access roles management; and evidence of periodic review of access roles and logs pertaining to critical systems.	
7	ICTY should design and implement procedures for tracking all the data associated with the acquisition and/or development of software applications in preparation for compliance with the IPSAS requirements for intangible assets.	Important	O	Receipt of documentation showing adequate recording and tracking of software-related data for compliance with IPSAS on intangible assets.	30 April 2014

APPENDIX I

Management Response

APPENDIX I

MANAGEMENT RESPONSE

Audit of information and communications technology management at the International Criminal Tribunal for the former Yugoslavia

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	ICTY should clarify: (a) the roles and responsibilities of the ICT Committee; and (b) the criteria for assessing ICT investments of MICT, in coordination with MICT.	Important	Yes	ICTY ICT Committee Chair	30 June 2014	ICTY will update and re-circulate the Committee's terms of reference. In addition, a proposal will be submitted to the MICT Registrar that he recognize the advice of the Committee, acting in a joint organizational capacity, to make recommendations to him on MICT ICT projects and related expenditure. Although MICT staff members have already been included in Committee deliberations, the MICT Registrar will be advised to officially appoint adequate MICT representation in the Joint ICT Committee. ICTY will continue to consult and coordinate as needed with the ICTR on an operational level for projects which require such coordination.
2	ICTY should revise and formally approve its ICT strategy in order to identify ICT priorities and the resources required for completing its mandate and transfer/support to MICT.	Important	Yes	Chief, ITSS	30 June 2014	ICTY will review and formally approve its ICT strategy
3	ICTY should improve ICT project	Important	Yes	Head of ITSS	30 June 2014	The ICT Committee will ensure that

[1] Critical recommendations address significant and/or pervasive deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance cannot be provided regarding the achievement of control and/or business objectives under review.
[2] Important recommendations address important deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

MANAGEMENT RESPONSE

Audit of information and communications technology management at the International Criminal Tribunal for the former Yugoslavia

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	management by strengthening the formulation of project proposals, project monitoring and reporting, and maintenance of project documentation for ICT projects.			Application and Life Cycle management Unit (ALMU) Head of ITSS Operations		(i) proposed projects are explicitly aligned with the adopted ICT Strategy; (ii) the benefits, resource costs and risks are stated in the Business Case (HLBC) prior to project consideration and approval. ICTY will also strengthen its use of the PRINCE2 project management methodology. As ICT projects vary in size and complexity, ITSS will maintain standard ICT project documentation at the level appropriate to the projects' size and complexity. The documentation which will be produced for each project will be standardised and documented at the beginning of the project and maintained by each project manager.
4	ICTY should establish a consolidated and updated catalogue of applications and procedures for its maintenance to facilitate closure arrangements and transfer of systems to MICT.	Important	Yes	Chief of ITSS	30 September 2014	ICTY will establish a consolidated and updated application portfolio. Procedures will be adopted which ensure that the established portfolio is maintained and current.
5	ICTY should ensure that ICT project proposals are subjected to information security reviews prior to their submission to the ICT Committee, to ensure compliance with information security guidelines.	Important	Yes	ICTY ICT Committee Chair	30 June 2014	The HLBC process will be modified to address this as part of the drafting process, and the template used for HLBCs will be amended to ensure that each HLBC is reviewed by the Information Security Officer prior to

APPENDIX I

MANAGEMENT RESPONSE

Audit of information and communications technology management at the International Criminal Tribunal for the former Yugoslavia

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						consideration by the ICT committee.
6	ICTY should strengthen access role management by: (a) reviewing the list of users with access to the Personnel Information Management System and the OneSource system and revoking the access rights granted to staff that no longer need to use the systems (b) implementing standard operating procedures for managing roles and credentials for accessing information systems during the movement of staff within the Tribunal; and (c) instituting periodic reviews of access roles and logs pertaining to critical systems and applications.	Important	Yes	Head, ITSS ALMU Head, ITSS Operations Unit Chief of ITSS	30 April 2014	(a) The list of users with access to the Personnel Information Management System and the OneSource system will be reviewed and appropriately amended with the HR and Procurement sections respectively. (b)All access roles (including all staff movement requests) are requested through Service Desk after approval from the business owner. ITSS has established a Standard Operating Procedure (SOP) which will be published and promulgated with all ICTY business owners and the ICTY Service Desk. The revised procedures detailed in this SOP will enable both ITSS and the business owners jointly to manage user access roles, and will detail the steps to be taken when the access roles of staff members need to be changed. (c) ITSS will review access roles list for critical systems and applications, at minimum every quarter, with business owners, and the results of the review will be documented and acted upon with minimal delay. Due to the larger amount of records automatically generated by the logs and resource overheads involved in re viewing these logs, the access logs will be reviewed only when required

APPENDIX I

MANAGEMENT RESPONSE

Audit of information and communications technology management at the International Criminal Tribunal for the former Yugoslavia

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						in the context of specific incidents. This, when combined with the new access control procedures instituted by the SOP, will strike the correct balance of risk mitigation to ensure that proper access role management is carried out.
7	ICTY should design and implement procedures for tracking all the data associated with the acquisition and/or development of software applications in preparation for compliance with the IPSAS requirements for intangible assets.	Important	Yes	Head, ITSS ALMU Head, ITSS Operations	30 April 2014	Software acquisition data will be recorded and tracked using Central Supplies System. The opening balances for acquisitions as of 1 January 2014 will be completed before 14 February 2014 as required for IPSAS compliance. For in-house developed software, ITSS will use the Time Tracking application to estimate the total development cost to ensure appropriate compliance with IPSAS requirements.

APPENDIX I

MANAGEMENT RESPONSE

Audit of information and communications technology management at the International Criminal Tribunal for the former Yugoslavia

Draft Audit Report	Management Response
Paragraph 22	
There were weaknesses in the formulation and implementation of the ICT strategy in that the strategy referred to generic organizational goals (i.e., completion of the ICTY mandate and support for transfer to MICT), but did not identify the related ICT priorities and resources. As a result, low priority projects in the context of the downsizing and impending closure of ICTY were completed during the audit period, while high priority projects proposed during the first half of 2012 were not. For example, the project for enhancements to the Office of Legal Aid Finance Tracking system, which projected a 30 percent reduction in processing time of invoices submitted by defence teams, was not completed, while the projects of the Tribunal's intranet re-design and implementation of free Wi-Fi in ICTY premises were completed. Also, although the overall resource requirements were quantified in the budget, there was no visible connection between the ICT strategy and the budget. The strategy identified discrete ICT projects whereas the budget quantified ICT resource requirements under various budget lines, mixing both new investments and the cost of providing day-to-day services. Further, the strategy was not reviewed on an annual basis, as required by the terms of reference of the ICTY ICT Committee. Periodic reviews were necessary to ensure the continued alignment of the strategy with the organization's mandate, business needs, shifting priorities, technological developments, and available resources.	ICTY would like to note that while it accepts some aspects of this observation, the conclusions drawn about project prioritization are over-simplified and incorrect. As explained during the audit, ICTY would like to reiterate that the reason for the Wi-Fi project being completed before the OLAD project is the fact that the two projects described here were of different scope and used two different sets of resources. The Wi-Fi project was a small one, which used inexpensive 'off-the-shelf' hardware and software, and since very minimal customization or configuration which required staff resources was needed, the project could be completed in a very short period. The OLAD project, while a high priority, required the use of staff resources which were also needed to work on the Comparative Review Portal, which was an urgent priority for the ICTY, especially with regards to the Completion Strategy. This meant that the Wi-Fi project could be realized in the short term, while the OLAD project had to be postponed, as they relied on distinct uncontended resources.
Paragraph 36	
ICTY accepted recommendation 6 and stated that the list of users with access to PIMS and the OneSource system will be reviewed and appropriately amended with the collaboration of Human Resources and Procurement Sections, respectively. ICTY also stated that it will publish a Standard Operating Procedure which will enable ITSS and the business owners jointly to manage user access roles. Additionally, ITSS will	ICTY will not undertake periodic review of the logs of critical systems unless there is a specific incident, as the systems produce so much data that reviewing the logs would consume most of the staffing resources currently assigned to the IT section. We would like to repeat the response we submitted in January 2014: "*Due to the larger amount of records automatically generated by the logs and resource overheads*

MANAGEMENT RESPONSE

Audit of information and communications technology management at the International Criminal Tribunal for the former Yugoslavia

review access roles lists for critical systems and applications, at minimum every quarter, with business owners, and the results of the review will be documented and acted upon with minimum delay. Due to the larger amount of records automatically generated by the logs and resource overheads involved in reviewing these logs, the access logs will be reviewed only when required in the context of specific incidents. Recommendation 6 remains open pending receipt of an amended list of users and access rights to PIMS and the OneSource system; of the published Standard Operating Procedure on access roles management; and evidence of periodic review of access roles and logs pertaining to critical systems.	*involved in reviewing these logs, the access logs will be reviewed only when required in the context of specific incidents.* *This, when combined with the new access control procedures instituted by the SOP, will strike the correct balance or risk mitigation to ensure that proper access role management is carried out."*
Paragraph 39	
The system used by ICTY for recording and controlling software licenses did not include relevant information for IPSAS compliance, such as cost (purchase price, import duties, and non-refundable taxes), units, and dates of purchase or use for measurement and reviewing impairment of individual licenses. Different criteria were used for recording the number of enterprise Original Equipment Manufacturer (OEM), site, and volume licenses. For example, in some cases the records showed the number of licenses, while in others the records showed the number of units (users or computers) that each license allowed.	ICTY does not believe that the various types of licenses are relevant to this observation. It is a fact that various software titles are sold and licensed on widely variable terms and conditions of licensing and usage, and we submit that the records kept accurately reflect those terms and conditions. We would like to request that these sentences be removed from the report as 1) it is presented that this practice is incorrect, and 2) it is not relevant to the observation.
Paragraph 40	
Inadequate recording and measurement of costs and usage of software licenses did not allow effective control and acquisition/disposal planning and did not meet requirements for IPSAS compliance after 1 January 2014. ICTY attributed the shortcoming to system limitations, difficulties in addressing different terminologies of vendor software packages and late issuance of guidance by the IPSAS Implementation Team at Headquarters, which resulted in lack of preparedness to deal with requirements on the reporting of intangible assets under IPSAS.	ICTY did not attribute our IPSAS compliance shortcomings to *"difficulties in addressing different terminologies of vendor software packages"* and so we would like this phrase to be removed.

…